Preservation Evidence Policy - Profile TR-ESOR V1.3 MAX using ERS

Table of Content

Versioning

Preservation Evidence Policy - Profile TR-ESOR V1.3 MAX using ERS

Version: 1.0, March 2024

Creation: on behalf of procilon GmbH

Table 1. Versioning

Version	Date	Description	Edited by
1.0	15.03.24	Initial Creation	H. Werner

1 Introduction

1.1 Overview

1.1.1 Purpose

The document describes the Preservation Evidence Policy (PEP) based on the Preservation Evidence Policy Template (PEPT) of the BSI [TR-ESOR-PEPT] provided by the manufacturer for the TR-ESOR-Product **ProNEXT Archive Manager**. To fulfill general requirements this document precises and is fulfilled with information about manufacturer relevant data about the product. In addition it is published.

1.1.2 Scope of the document

This PEP is about a system for the storage and preservation of cryptographically signed documents according to [TR-ESOR]. Such a system includes components and processes, which are used for:

1. The preservation over long periods of time, using: digital signature techniques, the abilities to validate a digital signature to maintain its validity status and to get a proof of existence of the associated signed data even if later the signing key becomes compromised the certificate expires or the signature algorithm becomes obsolescent.
2. The provision of a proof of existence of digital objects, whether they are signed or not, using digital signature techniques over long periods of time.

The TR-ESOR middleware is limited to functions, interfaces and components necessary for the preservation of evidence. Going beyond this is permissible, provided functions for preserving the value of evidence are not restricted. The TR-ESOR middleware includes neither custom applications nor storage systems. Securing the availability and readability of documents cannot guaranteed by the TR-ESOR middleware or its PEP, but must be supported by suitable technical and organisational measures in the upstream IT applications or storage systems used.

The following minimal functional requirements have to be fulfilled:

- the storage of cryptographically unsigned/signed data, possibly including already existing Evidence Records pursuant to [RFC4998]
- the retrieval of Archival Information Package (AIP)
- the retrieval of suitable Evidence Records of the authenticity and integrity of the stored data,
- the deletion of data as Archival Information Package,
- the traceable update of already archived metadata and payload data and credentials, which also includes the addition of further metadata and payload data to already archived data structures
- the verification of the Archival Information Package including the supplemental evidence data and technical evidence records (Evidence Records) that are contained therein or were additionally transferred
- the retrieval of Preservation Profiles

1.2 Document Name and Identification

This PEP is identified as follows:

- Title: Preservation Evidence Policy - Profile TR-ESOR V1.3 MAX using ERS
- Version: 1.0
- Identifier: 1.3.6.1.4.1.25676.40.1.1.1.1.0

The identifier corresponds to an ObjectIdentifier (OID) composed as follows

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) procilon GmbH(25676) tresor(40) pep(1) v1.3_MAX (1) ERS (1) major-version(1) minor-version(0)}

and documents conformity to corresponding specifications, in particular [TR-ESOR].

1.3 Preservation Participants

The participants of a TR-ESOR-Product are the following parties:

- the TR-ESOR-Product manufacturer
  - external Providers, i.e.
    - Validation Service
    - Time Stamping Authority
- user of the TR-ESOR-Product

1.4 Preservation Usage

This PEP is related to "Preservation product with storage [WST]" pursuant to [ETSI TS 119 511].

The TR-ESOR-Product is used to fulfil the following goals:

- provides proof of existence over long periods of time of the submission data object submitted
- extends over long periods of time the ability to validate a digital signature, to maintain its validity status and to get a proof of existence of the associated signed data
- supports the augmentation of submitted preservation evidences

1.5 Policy administration

This PEP is subject to continuous further improvement and adaptation to new requirements.

The continuation, in form of agreed versions of this PEP, are released in a formal act. Formally released versions are published in addition on the BSI website. The procilon GmbH is technically responsible for the formulation and supervision of this PEP an its versions.

The contact details of the procilon GmbH are:

procilon GmbH
Leipziger Straße 110
04425 Taucha b. Leipzig
Phone: +49 34298 4878-10
E-Mail: info@procilon.de
Internet: https://www.procilon.de

1.6 Definitions, acronyms and references

Table 2. Abbreviations

Abbreviation	Description
AOID	Archive Data Object Identifier
ASiC-AIP	Associated Signature Container (ASiC)
Archival	Information Package
ATS	ArchiveTimeStamp
AUG	Augmentation
CA	Certification Authority
CAB	Conformity Assessment Body
CRL	Certificate Revocation List
DMS	Data Management System
eIDAS-VO	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market and repealing Directive 1999/93/EC
ECM	Enterprise Content Management
EU	European Union
EUMS	European Union Member State
GDPR	General Data Protection Regulation
IS-Policy	Information Security Policy
IT	Information Technology
LXAIP	Logically XML formatted Archival Information Package
NC	Non-Conformity
OCSP	Online Certificate Status Protocol
OVR	Overall
OID	Object Identifier
PDS	Preservation of Digital Signature

Abbreviation	Description
PEP	Preservation Evidence Policy Template
PEP	Preservation Evidence Policy
PGD	Preservation of General Data
PI	Potential for Improvement
PO	Preservation Object
POC	Preservation Object Container
PP	Preservation Profiles
PRP	Preservation Service Protocol
PSP	Preservation Service Provider
PSPS	Preservation Service Practice Statement
PS	Preservation Service
QES	Qualified Electronic Signature or qualified electronic seal
QTSP	Qualified Trust Service Provider
QPSP	Qualified Preservation Service Provider
R	Recommendation
SSL	Secure Sockets Layer
SA	Subscriber Agreement
SubDO	Submission Data Object
SVP	Signature Validation Policy
T&C	Terms and Conditions
TL	Trusted List
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TS-Policy	Trust Service Policy
UTC	Coordinated Universal Time
WOS	Without Storage
WST	With Storage
WTS	With Temporary Storage
XAIP	XML formatted Archival Information Package
XML	Extensible Markup Language

Table 3. References

Reference	Description
[ETSI EN 319 162]	European Telecommunications Standards Institute (ETSI): Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers – Version 1.2.1. Verfügbar unter: https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf, Letzter Zugriff: 15.03.24
[ETSI EN 319 421]	European Telecommunications Standards Institute (ETSI): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps – Version 1.2.1. Verfügbar unter: https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf, Letzter Zugriff: 15.03.24
[ETSI TS 119 312]	European Telecommunications Standards Institute (ETSI): Cryptographic Suites – Version 1.4.3. Verfügbar unter: https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf, Letzter Zugriff: 15.03.24
[ETSI TS 119 511]	European Telecommunications Standards Institute (ETSI): Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques – Version 1.1.1. Verfügbar unter: https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf, Letzter Zugriff: 15.03.24
[ETSI TS 119 512]	European Telecommunications Standards Institute (ETSI): Protocols for trust service providers providing long-term data preservation services – Version 1.2.1. Verfügbar unter: https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.02.01_60/ts_119512v010201p.pdf, Letzter Zugriff: 15.03.24
[RFC4998]	Internet Engineering Task Force (IETF): RFC 4998 - Evidence Record Syntax (ERS). Verfügbar unter: https://tools.ietf.org/html/rfc4998, Letzter Zugriff: 15.03.24
[SOG-IS]	SOG-IS Crypto Working Group: SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms - Version 1.3 February 2023. Verfügbar unter: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf, Letzter Zugriff: 15.03.24
[TR-KRYPT]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-02102 – Kryptographische Verfahren - Version 2024-01: Empfehlungen und Schlüssellängen. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, Letzter Zugriff: 15.03.24

Reference	Description
[TR-ESOR]	Bundesamt für Sicherheit in der Informationstechnik (BS I): TR-03125 – Beweiswerterhaltung kryptographisch signierter Dokumente. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24
[TR-ESOR-ERS]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-03125 – Profilierung der Evidence Records gemäß RFC4998 und RFC6283 – Version 1.3. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24
[TR-ESOR-F]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-03125 – Formate - Version 1.3. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24
[TR-ESOR-M.2]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-03125 – Formate – Version 1.3. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24
[TR-ESOR-M.3]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-03125 – ArchiSig-Modul – Version 1.3. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24
[TR-ESOR-PEPT]	Bundesamt für Sicherheit in der Informationstechnik (BSI): TR-03125 – Preservation Evidence Policy Template – Version 1.3. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html, Letzter Zugriff: 15.03.24

2 Publication and Repository Responsibilities

2.1 Repositories

The valid version of this PEP is available for download on the website of the procilon GmbH at: https://www.procilon.de/pronext-archive-manager/preservation_evidence_policy.pdf .

The PEP document contains a description of changes and the dates when the changes took place.

The valid version of the used PP is available for download on the website of procilon GmbH at: https://www.procilon.de/pronext-archive-manager/preservation_profile.xml .

2.2 Storage of preservation evidences or publication of the preservation evidence policy

The TR-ESOR-Middleware is responsible for the preservation of evidences of documents based on Evidence Records based on Merkle-Hash-treed defined in [RFC4998].

The ArchiSig-Module uses a secure data storage, that is part of or allocated to the ArchiSig-Module, to store the ArchiveTimeStamp and the archive data object ID in a way, that concerning the hash trees a hash value corresponding to an AOID and VersionID can be identified with absolute certainity at any time.

2.3 Time or frequency of publication

This PEP administration follows a standardised and regular process. It can only be edited and published from authorized personnel of the procilon GmbH.

A change or update of the actual PEP version at least will take place, if

- a new version of [TR-ESOR] is published,
- used cryptographic algorithm(s) and its parameter(s) have to be changed.

3 Identification and Authentication

3.1 Naming

Not applicable.

3.2 Initial identity validation

Not applicable.

3.3 Identification and Authentication for modification requests

Not applicable.

3.4 Identification and Authentication for deleting requests

Not applicable.

4 Preservation Service Life-Cycle Operational Requirements

4.1 Preservation Service Application

Not applicable.

4.2 Preservation Service application processing

Not applicable.

4.3 Preservation Evidence Record issuance

The TR-ESOR-Middleware creates Preservation Evidence Records pursuant to [RFC4998].

Algorithms are chosen on base of [ETSI TS 119 312], [SOG-IS] and [TR-KRYPT].

4.4 Preservation Evidence Record acceptance

The TR-ESOR-Middleware validates Preservation Evidence Records pursuant to [RFC4998].

4.5 Preservation Object modification

Not applicable.

4.6 Preservation Evidence Record usage

Not applicable.

4.7 Preservation Evidence Record renewal

The TR-ESOR-Middleware augments Preservation Evidence Records pursuant to [RFC4998] by time-stamp renewal and hash-tree renewal. How this is performed is specified in chapter 5 of [RFC4998]. The algorithms chosen for Preservation Evidence Record renewal are shown in section 7.7.4.

4.8 Preservation Export-Import

Section 2.7 of [TR-ESOR-M.3] describes different methods with different Export-Import data formats with different interfaces for exporting and importing export-import package(s). The alternatives supported by the TR-ESOR-Product Manufacturercan be found in section 7.7.6.

4.9 Certificate re-key

Not applicable.

4.10 Preservation Data Deletion

Not applicable.

4.11 Preservation Status Services

Not applicable.

4.12 Key escrow and recovery

Not applicable.

4.13 End of subscription

Not applicable.

5 Facility, Management and Operational Controls

5.1 Physical controls

Not applicable.

5.2 Procedural controls

Not applicable.

5.3 Personnel controls

Not applicable.

5.4 Audit logging procedures

The TR-ESOR-Middleware offers comprehensive and configurable options for logging, which allow to log information, warnings and errors during the operation of the modules.

The messages are forwarded to the logging system via so-called loggers. Corresponding configuration parameters are provided for this purpose. The settings for the logging system are stored in configuration files.

Only authorized administrators familiar with the user manual have access to the configuration of the logging system and to the log files themselves.

In the configuration, the output can be filtered depending on the importance of the message. The output scope increases with the assigned importance level and includes all messages of the level itself as well as all even more urgent levels.

The order of log levels is as follows: ALL > TRACE > DEBUG > INFO > WARN > ERROR > FATAL > OFF

The following information classified by importance is provided:

ALL - all messages are output unfiltered
TRACE - more detailed debugging, comments
DEBUG - general debugging
INFO - general information
WARN - occurrence of an unexpected situation
ERROR - errors
FATAL - critical error, program abort
OFF - logging is disabled

Access to the log files is secured via the system and user rights (therefore: at least SSH login + setting appropriate permissions).

5.5 Records archival

Not applicable.

5.6 Algorithm changeover

Not applicable.

5.7 Compromise and disaster recovery

Not applicable.

5.8 Preservation Service termination

Not applicable.

5.9 End of the Preservation Period

Archived data objects can be deleted after the preservation period is expired. In contrast to archived objects whose retention period has not yet expired, no special reason for the deletion needs to be given. c Archived data objects are preserved beyond the expiration of retention periods by default. This means that there are no regular checking runs for expired retention periods with subsequent automatic deletion of data. Any requirements in this regard is to be implemented on a customer-specific basis.

6 Technical Security Controls

6.1 TR-ESOR Modules

Not applicable.

6.2 Private Key Protection and Cryptographic Module

Not applicable.

6.2.1 Private Key Protection

Not applicable.

6.2.2 Protection of the Cryptographic Module

Not applicable.

6.2.3 Configuration of the Cryptographic Module

Not applicable.

6.3 Other aspects of key pair management

Not applicable.

6.4 Activation data

Not applicable.

6.5 Computer security controls

Not applicable.

6.6 Life cycle technical controls

Not applicable.

6.7 Network security controls

Not applicable.

6.8 Time stamping

Not applicable.

7 Formats and Profiles

7.1 Algorithm change

Based on monitoring the TR-ESOR-Middleware reacts before expiration of the security suitability of used algorithms and related parameters. Used algorithms are based on [ETSI TS 119 312], [SOG-IS] and [TR-KRYPT]. The Crypto Module supports fast and easy exchange of algorithms and parameters.

The TR-ESOR-Middleware performs time-stamp or hash-tree renewals as specified in [RFC4998]. Therefore the ArchiSig Module have got a secondary data basis. The secondary data basis of the ArchiSig Module uses other algorithm and parameters as the primary data basis. Nevertheless, a fast and easy algorithm change is guaranteed too.

7.2 Preservation Profile

In context of [TR-ESOR] the following Preservation Profiles exists:

1. TR-ESOR V1.2.1/V1.2.2 with the TR-S.4-Interface:
   a. BSI-TR-ESOR-v1.2.1-S4-Profile.xml with the identifier:
   http://www.bsi.bund.de/tr-esor/V1.2.1/profile/S.4/v1.0
   b. BSI-TR-ESOR-v1.2.2-S4-Profile.xml with the identifier:
   http://www.bsi.bund.de/tr-esor/V1.2.2/profile/S.4/v1.0
   c. BSI-TR-ESOR-v1.3-S4-Profile.xml with the identifier:
   http://www.bsi.bund.de/tr-esor/V1.3/profile/S.4/v1.0_MAX or
   http://www.bsi.bund.de/tr-esor/V1.3/profile/S.4/v1.0_MIN
   or
2. TR-ESOR V1.2.1/V1.2.2 with the TS 119 512-Interface TR-512 together with or without the “ETSI TS119512 TR-ESOR Transformator”:
   a. BSI-TR-ESOR-v1.2.1-ETSI-TS-119512-v1.1.2-Profile.xml with the identifier
   http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/v1.1.2
   NOTE: Only with the “ETSI TS119512 TR-ESOR Transformator”
   b. BSI-TR-ESOR-v1.2.2-ETSI-TS-119512-v1.1.2-Profile.xml with the identifier
   http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/v1.1.2
   c. BSI-TR-ESOR-v1.3-ETSI-TS-119512-v1.1.2-Profile_MAX_LOCAL.xml with the identifier
   http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/v1.1.2_MAX
   or BSI-TR-ESOR-v1.3-ETSI-TS-119512-v1.1.2-Profile_MIN_LOCAL.xml
   http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/v1.1.2_MIN

7.2.1 Profile identifier http://www.bsi.bund.de/tr-esor/V1.2.1/profile/S.4/v1.0

Not applicable.

7.2.2 Profile identifier http://www.bsi.bund.de/tr-esor/V1.2.2/profile/S.4/v1.0

Not applicable.

7.2.3 Profile identifier http://www.bsi.bund.de/tr-esor/V1.3/profile/S.4/v1.0_MAX

This is the Preservation Profile used by the TR-ESOR-Product: TR-ESOR V1.3 MAX with the TR-S.4-interface, created on 15th of March 2022, modified by specifying the used evidence record format [RFC4998], validation policies and removing the optional operation ArchiveTrace.

Listing 1. Preservation Profile TR-ESOR V1.3 MAX using ERS

```
<?xml version="1.0" encoding="UTF-8"?>
<pres:Profile xmlns:pres="http://uri.etsi.org/19512/v1.1.2#"
xmlns:md="http://docs.oasis-open.org/dss-x/ns/metadata"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://uri.etsi.org/19512/v1.1.2# ./19512-Preservation-
API_V.1.1.2.xsd">
    <!-- ================================================== -->
    <!-- Profile of BSI-TR-ESOR-S.4-V1.3 Interface (MAX)    -->
    <!-- ================================================== -->
    <!-- Version of 15.03.2022 modified by manufacturer     -->
    <!-- ================================================== -->
    <md:ProfileIdentifier>http://www.bsi.bund.de/tr-
esor/V1.3/profile/S.4/v1.0_MAX</md:ProfileIdentifier>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
    <md:Description xml:lang="DE">Dieses Profil beschreibt die TR-S.4 Schnittstelle
gem. BSI-TR-ESOR V1.3 in deren maximalen Ausprägung - modifiziert vom Hersteller des
TR-ESOR-Produkts.</md:Description>
    <md:Operation>
        <md:Name>ArchiveSubmission</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.1</md:Description>
        <md:Input>
            <md:Name>ArchiveSubmissionRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.1.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>ArchiveSubmissionResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.1.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveUpdate</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
```

```
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.2</md:Description>
        <md:Input>
            <md:Name>ArchiveUpdateRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.2.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>ArchiveUpdateResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.2.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveRetrieval</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.3</md:Description>
        <md:Input>
            <md:Name>ArchiveRetrievalRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.3.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>ArchiveRetrievalResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.3.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveEvidence</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.4</md:Description>
        <md:Input>
            <md:Name>ArchiveEvidenceRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.4.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>ArchiveEvidenceResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.4.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveDeletion</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.5</md:Description>
        <md:Input>
            <md:Name>ArchiveDeletionRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.5.1</md:Description>
        </md:Input>
```

```
        <md:Output>
            <md:Name>ArchiveDeletionResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.5.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>Verify</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.7</md:Description>
        <md:Input>
            <md:Name>VerifyRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.7.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>VerifyResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap 3.7.2</md:Description>
        </md:Output>
    </md:Operation>
    <md:Operation>
        <md:Name>RetrieveInfo</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.8</md:Description>
        <md:Input>
            <md:Name>RetrieveInfoRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.8.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>RetrieveInfoResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.8.2</md:Description>
        </md:Output>
    </md:Operation>
    <!-- The following operations are optional. Please delete the following
operations, if not supported.   -->
    <md:Operation>
        <md:Name>ArchiveData</md:Name>

<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_3.pdf</md:Specification>
        <md:Description xml:lang="DE">Siehe Kap. 3.6</md:Description>
        <md:Input>
            <md:Name>ArchiveDataRequest</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.6.1</md:Description>
        </md:Input>
        <md:Output>
            <md:Name>ArchiveDataResponse</md:Name>
            <md:Description xml:lang="DE">Siehe Kap. 3.6.2</md:Description>
        </md:Output>
```

```
    </md:Operation>
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
    <!-- The signature policy chosen by the TR-ESOR-product manufacturer. -->
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
    <!-- The timestamp policy chosen by the TR-ESOR-product manufacturer. -->
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
    <pres:SchemeIdentifier>
http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers</pres:SchemeIdentifier>
    <pres:ProfileValidityPeriod>
        <pres:ValidFrom>2022-05-04T00:00:00Z</pres:ValidFrom>
    </pres:ProfileValidityPeriod>
    <pres:PreservationStorageModel>WithStorage</pres:PreservationStorageModel>
    <!-- TR-ESOR supports all three Preservation Goals -->
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pds</pres:PreservationGoal>
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pgd</pres:PreservationGoal>
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/aug</pres:PreservationGoal>
    <pres:EvidenceFormat>
        <md:FormatID>urn:ietf:rfc:4998</md:FormatID>
        <md:Specification>https://ietf.org/rfc/rfc4998.txt</md:Specification>
    </pres:EvidenceFormat>
</pres:Profile>
```

The Preservation Profile can be retrieved by using the operation RetrieveInfo.

7.2.4 Profile ID http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/v1.1.2

Not applicable.

7.2.5 Profile ID http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/v1.1.2

Not applicable.

7.2.6 Profile ID http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/v1.1.2

Not applicable.

7.3 XML Scheme

See attachment of [TR-ESOR-F].

7.4 Archival Information Package (Container)

7.4.1 Archival Information Package (Container) Formats

The Archival Information Package Container Type “XAIP” is supported. In addition the Archival Information Package Container Type “LXAIP” is supported. The default Archival Information Package Container type is “XAIP”.

The following ArchiveData-Element Types are supported:

a. CAdES pursuant to [ETSI TS 119 512]

b. XAdES pursuant to [ETSI TS 119 512]

c. PAdES pursuant to [ETSI TS 119 512]

d. ASiC-E pursuant to [ETSI TS 119 512]

e. ASiC-S pursuant to [ETSI EN 319 162]

f. Binary Data (BIN) as Octet Stream, which is stored in the ECM-/Long-Term Storage by an “Upload-Request”, but only if connected with a corresponding LXAIP.

Table 4. Currently usable Archival Information Package and ArchiveData-Element Type(s)

Archival Information Package and ArchiveData-Element types	**Archival Information Package and ArchiveData-Element types in use by TR-ESOR-Product Manufacturer**
LXAIP	Is supported by the TR-ESOR-Product.
ASiC-AIP	Is not supported by the TR-ESOR-Product.
CAdES	Is supported by the TR-ESOR-Product.
XAdES	Is supported by the TR-ESOR-Product.
PAdES	Is supported by the TR-ESOR-Product.
DigestList	Is not supported by the TR-ESOR-Product.
ASiC-E	Is supported by the TR-ESOR-Product.
ASiC-S	Is supported by the TR-ESOR-Product.
Binary Data	Is supported by the TR-ESOR-Product.

7.4.2 XAIP

See section 3.1 of [TR-ESOR-F].

7.4.3 LXAIP

See section 3.2 of [TR-ESOR-F].

7.4.4 ASiC-AIP

Not applicable.

7.4.5 Validation of Archival Information Package (Container)

Formats according to Annex F of [TR-ESOR-F] and [RFC4998], cryptographic algorithms according to section 5.2 of [TR-ESOR-ERS] based on [ETSI TS 119 312], [SOG-IS] and [TR-KRYPT] are used.

7.5 Payload Data Formats

Formats according to chapter 4 of [TR-ESOR-F] are used.

7.6 Cryptographic Data Formats

Formats according to chapter 5 of [TR-ESOR-F] are used.

7.7 Evidence Record Format

7.7.1 Generation

The Evidence Record is generated according to [RFC4998] and contains no explicit information of the Preservation Evidence Policy or the Preservation Profile.

Table 5. Used Preservation Evidence Record Type

Evidence Record Type	Evidence Record Type in use by the TR-ESOR-Product Manufacturer
[RFC4998]	Is in use by the TR-ESOR-Product Manufacturer.

Cryptographic algorithms according to section 5.1 of [TR-ESOR-ERS] based on [ETSI TS 119 312], [SOG-IS] and [TR-KRYPT] are used.

Table 6. Algorithms in Use for the generation of timestamp token

Crypto-Function Type	Algorithms in use by the TR-ESOR-Product Manufacturer
Hash function	SHA-256, SHA-384, SHA-512
TST signature algorithm	RSA PSS with key lengths of 3072, 4096 bit

The hash algorithms to be used may be specified by the TSP. TSPs used in individual cases to retrieve qualified electronic time stamps may depend in particular on customer-specific configuration.

7.7.2 Validation

Evidence Record

Cryptographic algorithms according to section 5.2 of [TR-ESOR-ERS] based on [ETSI TS 119 312], [SOG-IS] and [TR-KRYPT] are used.

Table 7. Algorithms in Use for the verification of timestamp token

Crypto-Function Type	Algorithms in use by the TR-ESOR-Product Manufacturer
Hash function	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-160
TST signature algorithm	RSA PKCS#1 v.1.5 and RSA PSS with key lengths of 2048, 3072, 4096 bit

ArchiveTimeStamp

See section 4.3 of [RFC4998].

ArchiveTimeStampSequence and ArchiveTimeStampChain

See section 5.3 of [RFC4998].

7.7.3 Applicable Trust Service Provider ((Q)TSP)

The following external TSP are used by the TR-ESOR-Middleware:

- Time Stamping Authority issuing qualified timestamps

A signature is not created by the TR-ESOR-Middleware, when creating a preservation evidence.

Time Stamping Authority issuing qualified timestamps

The TR-ESOR-Middleware requests qualified time-stamps from a qualified Trust Service Provider conform to [ETSI EN 319 421] to create or augment an Evidence Record with ArchiveTimeStamps or ArchiveTimeStamp Chains or ArchiveTimeStamp Sequences pursuant to [RFC4998]. For the retrieval of timestamps, a secure communication communication channel to the trusted service provider is established if the trusted service provider supports this.

In principle, all qualified Timestamp Trust Service Providers which are listed on the European Trusted List and which are also assigned the status 'granted' can be configured for requesting timestamps.

The qualified Trust Service Provider used may depend on the customer-specific configuration.

Table 8. Trust Anchor of the external Timestamp Trust Service Provider

Certificate Field	**Certificate Field Value of the Trust Anchor**
Trust Anchor of the Trusted List	
subject	CN = EUROPEAN COMMISSION, E = digit-dmo@ec.europa.eu, O = EUROPEAN COMMISSION, 2.5.4.97 = LEIXG-254900ZNYA1FLUQ9U393, OU = Directorate-General for Digital Services (DIGIT), C = LU
issuer	CN = DIGITALSIGN QUALIFIED CA G1, O = DigitalSign Certificadora Digital, C = PT
serial number	73c21c494b5510a00c32f1e6f50594d39917b0f5
validity	2023-11-17 11:11:46 UTC - 2027-11-17 11:11:46 UTC
publiy key length	4096
signature algorithm	sha512WithRSAEncryption
SHA-256 fingerprint	d23011e04dba0769a059bc9ffb4b51af75eaa04de797ea573b2f470d555343a1
Link to the TL	https://ec.europa.eu/tools/lotl/eu-lotl.xml

Validation Service for (qualified) electronic signatures, seals or timestamps

Not applicable.

Certificate Status Authority(ies) to validate certificates

Not applicable.

7.7.4 Augmentation of Evidence Record

The augmentation of Evidence Records is achieved by time-stamp renewal and hash-tree renewal. For the data formats and processing procedures used see section 5.2 of [RFC4998].

Algorithms to be used or requested for the hashtree renewal or the retrieval of timestamps can be easily changed by adjusting the corresponding parameters in the configurations of the ArchiSig and Crypto module.

Table 9. Algorithms in use for the time-stamp renewal and hash-tree renewal

Crypto-Function Type	Algorithms in use for the time-stamp renewal and hash-tree renewal
Hash function	SHA-256, SHA-384, SHA-512
TST signature algorithm	RSA PKCS#1 v.1.5 and RSA PSS with key lengths of 3072, 4096 bit

The algorithms to be used (in particular in requested timestamps) may be specified by the TSP. TSPs used in individual cases to retrieve qualified electronic time stamps may depend in particular on customer-specific configuration.

7.7.5 Validation of Digital Signatures

Verify or ValidateEvidence

For further processing it is necessary that at least one of both validation models (shell or chain) is successful. If both validation models (shell and chain) fail, it proceeds as follows: the ArchiSafe Module returns an understandable error message to the application and rejects the archiving of the object.

The function to verify digital signatures and thus time-stamps and certificates is provided by the Crypto Module. The hash algorithms SHA-1, SHA-224, SHA-256, SHA-384, RIPEMD-160 are supported for signature verification. Furthermore, the algorithms RSA PKCS#1 v.1.5 and RSA PSS with the key lengths 2048, 3072 and 4096 bit are permitted for signature verification.

The Crypto Module manages a catalog of algorithms that conforms to the DSSC standard. This allows essential algorithms such as hash algorithms to be supported to be specified according to their validity periods. Definitions are supplied with the Crypto Module [TR-ESOR-M2] that are used to specify, among other things, the cryptographic functions and algorithms to be used. Definitions for the validity of cryptographic algorithms are also supplied. These contain usable hash algorithms and can be updated within a few days by patch or update.

A list of trusted certificates may be configured for the Crypto Module.

Trust Anchor and Signature/Timestamp Validation Policy

The following validation policies are currently used for validation processes:

Table 10. Declaration of the „signature/timestamp validation policy“ used

Declaration of the „signature/timestamp validation policy“ used			
http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip	Yes	No	Description
	[x]	[]	See following text.
http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp	Yes	No	Description
	[x]	[]	See following text.

All signature related objects (e.g. electronic signatures / time-stamps, certificates, revocation lists, OCSP responses) contained in the XAIP or LXAIP container are verified up to a trustworthy root certificate or trust anchor. All verified electronic signatures / time-stamps contained in the XAIP or LXAIP container are supplemented with all the validation data, obtained in doing the verification.

The validation data (e.g. certificates, certificate revocation lists, OCSP responses) is stored as unsigned attributes or properties in the corresponding digital signatures or time-stamps or in the xaip:certificateValues or xaip:revocationValues sub-elements linked to the corresponding digital signatures or time-stamps. If the element ReturnVerificationReport is submitted in a Verify-request or ValidateEvidence-request, then the created verification report(s) are stored in the child-element vr:VerificationReport of the credential-Element of the XAIP or LXAIP.

All certificates and revocation information of a time-stamp validation are validated up to a trustworthy root certificate or trust anchor. If the timestamp does not meet the ETSI requirements, the check is aborted with a negative result and no further checks are carried out on the certificates.

If the Preservation Policy and the element ReturnVerificationReport is submitted in a Verify-request or ValidateEvidence-request, then all certificates and revocation information of a timestamp validation up to a trustworthy root certificate or trust anchor are verified. Information obtained for verifcation and created verification reports are inserted in the child-element vr:VerificationReport of the credential-Element of the XAIP or LXAIP.

Unsigned Data and Documents

Unsigned data is generally not treated differently than signed data. This applies in particular to their delivery, basic checking and storage. This includes the generation of an electronic archive entry hash value and an electronic archive entrytimestamp for the archive object. Due to the lack of signatures on the delivered data, no corresponding checks are performed.

7.7.6 Process of Export and Import of Export-Import-Packages

For the process of requesting export-import package(s) from the ECM-/long-Term-Storage, the following method is supported: Export-Import of (L)XAIPs with the integrated reduced Evidence Records.

Table 11. Details of Export and Import of Export-Import-Packages

Details of Export and Import of Export-Import-Packages	
Choice of export-import method pursuant to [TR-ESOR-M.3], clause 2.7 (A2.7-1)	Alternative 1a: Usage of ArchiveRetrieval or ArchiveEvidence functions to export archive data objects, usage of Verify function to determine evidence record data and usage of ArchiveSubmission or ArchiveUpdate functions to import archive data objects.
Choice of Export-Import data structure: a set of (L)XAIPs with reduced EvidenceRecords pursuant to [TR-ESOR-F]	Is in use by the TR-ESOR-Product Manufacturer.
Choice of how the request for an export-import package can be done	The concrete implementation of import-export is the responsibility of the clients or applications accessing the TR-ESOR middleware using existing functions and interfaces.

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of assessment

Not applicable.

8.2 Identity/qualifications of assessor

Not applicable.

8.3 Assessor’s relationship to assessed entity

Not applicable.

8.4 Topics covered by assessment

Not applicable.

8.5 Actions taken as a result of deficiency

Not applicable.

8.6 Communication of results

Not applicable.

9 Other Business and legal Matters

9.1 Fees

Not applicable.

9.2 Financial responsibility

Not applicable.

9.3 Confidentiality of business information

Not applicable.

9.4 Privacy of personal information

Not applicable.

9.5 Intellectual property rights

Not applicable.

9.6 Representations and warranties

Not applicable.

9.7 Disclaimers of warranties

Not applicable.

9.8 Limitations of liability

Not applicable.

9.9 Indemnities

Not applicable.

9.10 Term and termination

Not applicable.

9.11 Individual notices and communications with participants

Not applicable.

9.12 Amendments

Not applicable.

9.13 Dispute resolution provisions

Not applicable.

9.14 Governing law

Not applicable.

9.15 Compliance with applicable law

Not applicable.

9.16 Miscellaneous provisions

Not applicable.

9.17 Other provisions

Not applicable.